REMARKS

This Amendment and Response is filed in reply to the Office Action dated July 2, 2004. In this Response, Applicants traverse the Examiner's rejections of claims 1-17. Silence with regard to any of the Examiner's rejections is not an acquiescence to such rejections. Specifically, silence with regard to Examiner's rejection of a dependent claim, when such claim depends from an independent claim that Applicants consider allowable for reasons provided herein, is not an acquiescence to such rejection of the dependent claim(s), but rather a recognition by Applicants that such previously lodged rejection is moot based on Applicants' remarks and/or amendments relative to the independent claim (that Applicants consider allowable) from which the dependent claim(s) depends. Furthermore, amendments to the claims are being made solely to expedite prosecution of the instant application. Applicants reserve the option to further prosecute the same or similar claims in the instant or a subsequent application.

Upon entry of the Amendment, claims 1-17 are pending in the present application. The issues of the July 2, 2004 Office Action are presented below with reference to the Office Action.

With regard to the Office Action, paragraphs 1-3, "Claim Rejections - 35 USC §103:

The Examiner rejected claims 1, 2, and 7-14 under 35 U.S.C. §103(a) as being unpatentable over Davis et al. (U.S. Patent No. 6,367,009) in view of McNabb (U.S. Patent No. 6,289,462). The Examiner also rejected claims 4-6, 16, and 17 under 35 U.S.C. 103(a) as being unpatentable over Davis et al. in view of McNabb and further in view of Ginzboorg et al. (U.S. Patent No. 6,240,091), and rejected claims 3 and 15 under 35 U.S.C. 103(a) as being unpatentable over Davis et al. in view of McNabb and further in view of Grimmer (U.S. Patent No. 5,774,552).

As Examiner knows, and based at least on MPEP 2143, a *prima facie* case of obviousness under 35 U.S.C. 103(a) requires (1) a suggestion or motivation in the references themselves or generally known in the art, to combine the references, (2) a reasonable expectation of success to combine, and (3) *a teaching, via the combination, of all the claimed limitations* [emphasis added].

Applicants' independent claim 1 discloses an access system for a computer site, comprising a certificate authentication component to verify a user's identity from a digital certificate supplied by the user, *a directory, coupled to the certificate authentication component, to maintain an account for each user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, and an access control system, coupled to the directory, for controlling access to the computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the user in the directory.*

Davis describes a system and method for delegating authority and authentication from a client to a server (referred to as a middle-tier server, or MTS) so that the server can establish a secure connection to a back-end application on an end-tier server ("ETS") on behalf of the client, using the Secure Sockets Layer ("SSL") network protocol, or some other similar protocol (see abstract). More particularly, Davis proposes several techniques for extending SSL, or a like protocol, into a three-tier architecture in which the MTS establishes a secured connection with the ETS while being able to identify the true identity of the client, notwithstanding that the client is not directly connected to the ETS (generally, an intermediate server cannot establish a secured connection on behalf of a third party since the intermediate server does not have the third party's private key that is typically necessary to establish a secured connection).

Applicants agree with the Examiner's statement that Davis does not disclose permitting the user access to a portion of a computer site and restricting the user from at least one other portion of the computer site, and that Davis does not disclose user accounts indicating which portion of the computer site to which the corresponding user is permitted access (page 3, lines 3-6 of the Office Action). Applicants, however, respectfully disagree with the Examiner's proposition that McNabb discloses a system in which a user account is given an authorization attribute indicating access to a portion of a computer site and restricting the user from at least one other portion of the computer site.

McNabb describes a secured system and a modified operating system design where the access, control, rights and privileges are assigned to individual processes/files/objects being

accessed and not strictly to the user or process that accesses the computer (col. 1, lines 11-15). More particularly, McNabb describes an operating system for the trusted server that assigns and attaches to each of the server's processes, data objects, and data access requests, attributes that are subsequently used to control the access and use of those processes, objects, and requests (col. 8, line 54 to col. 9, line 33). Amongst the attributes that McNabb assigns and attaches are sensitivity labels (representing the security level associated with a process/object/data), privilege attributes (enabling processes/objects/requests to bypass certain security mechanisms), etc. (col. 8, lines 33-38, col. 9, lines 52-62, Figs. 2-3). Data access requests received at the trusted server are processed by an Advanced Secure Networking (ASN) component that assigns the request a sensitivity label based, in part, on the IP address associated with the request (col. 11, lines 18-28). An Upgrade/Downgrade Enforcer (UDE) module subsequently examines the request and redirects it to the appropriate service based on the ASN applied label of the request, the resource requested, and optionally the presence of authenticating certificates associated with the request (col. 11, lines 29-38). Thus, McNabb, in general, determines the type of access that should be provided to a resource based on the security and access attributes of the requested resource, and on the security attributes assigned to the request.

Although McNabb additionally discloses that a user may obtain access to individual components in the trusted server file system based on the user's personal access authorization privileges, and the user roles (e.g., anonymous user, system administrator, etc.), McNabb does not disclose a *directory to maintain an account for each user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access*, nor does McNabb disclose *an access control system, coupled to the directory for controlling access to the computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the user in the directory*. Rather, McNabb maintains a table of processes and/or data objects/files that are associated with user roles and privileges. The type of access a user will therefore be granted to a particular process or object will depend on whether, and to what extent, the user's role or authorization privilege matches the role and/or authorization privilege associated with the process (col. 6, lines 1-10, and col. 18, lines 1-40). For example, if a particular trusted server process allows only users having a specific authorization privilege to access and use that process, users not having this

specific authorization privilege will not be allowed access to that process. Similarly, in column 18, lines 53-63, which the Examiner referred to in the office action, a particular database row will be accessible to those users whose authorization level matches the authorization level for that database row. As described in lines 56-60: "Each row of a database table may have an extended attribute reflecting the authorization level or role that is required to view the record". Thus, whereas Applicants' claim 1 uses a directory of user accounts to specify the nature of the access each individual user is entitled to, McNabb, in contrast, specifies for each process and/or data object/file the types of users that are allowed access thereto.

Accordingly, since the combined teaching of Davis and McNabb does not teach a *directory to maintain an account for each user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access*, and *an access control system, coupled to the directory for controlling access to the computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the user in the directory*, as recited in Applicants' independent claim 1, Examiner fails to provide a *prima facie* case of obviousness for at least for failing to show all the elements of the claimed invention in the combined teaching cited by the Examiner, as required by MPEP 2143.

Moreover, Applicants submit that Examiner also fails to provide a *prima facie* case of obviousness for failing to provide a suggestion or motivation for combining the references cited by the Examiner, as required by MPEP 2143. As noted in MPEP 2143.01:

> Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art. "The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art." *In re Kotzab*, 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000).

As noted above, Davis is directed to a system and method for establishing a secured connection in a three-tier architecture between a client server, connected to a middle-tier server, and an end-tier server, also connected to the middle-tier server, but not directly connected to the client server. As such, Davis is concerned with communications between servers, and not about server management. Although Davis describes how authenticated files and/or data objects are created for the purpose of establishing a secured connection between the client server and the end-tier server, and how the authentication process is performed, Davis does not describe the intricate working of the operating systems running on any of the servers involved in establishing the secured connection between the three servers. While Davis discloses the use of a simple access control system to restrict access to users whose names are maintained on a list of authorized users, the Davis access control system does not involve elaborate access control mechanisms and techniques based on controlling access to processes, files, and other data objects.

In stark contrast, McNabb is directed to a system for managing and controlling user access to processes and data objects on a single trusted server, and describes an elaborate access control mechanism implemented as part of a modified operating system running on the trusted server. McNabb is not concerned with communications between servers, but rather deals exclusively with the management of a server's resources, which is accomplished by assigning authorization and access attributes to processes, files and other data objects.

Thus, since each of Davis and McNabb deal with entirely different and disparate technological issues (secured network communication vs. server resource management), and moreover, since McNabb describes a type of operating system implementation that Davis does not contemplate and which would require significant changes to the way the Davis is implemented were the server described in McNabb combined with the Davis system, no explicit or implicit motivation for combining the references by a person skilled in the art can be found in either of the references. Applicants thus submit that the Examiner failed to provide a *prima facie* case of obviousness for also failing to provide a suggestion or motivation for combining Davis and McNabb.

Since Applicants consider that the Examiner failed to provide a *prima facie* case of obviousness with respect to independent claim 1 for at least for failing to provide a suggestion or motivation for combining Davis with McNabb, and/or for failing to show all the elements of the claimed invention in the combined teaching of Davis and McNabb, Applicants thus traverse Examiner's 35 U.S.C. 103(a) rejection of independent claim 1, and consider independent claim 1 to be allowable. Claims 2-7 are also allowable as depending from an allowable base claim.

Independent claims 8 and 13 are method and system claims, respectively, describing features similar to those described in Applicants' independent system claim 1, including, for example, the use of a *directory*, or similar means, to maintain *an account for each user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access*, and *controlling access to the computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site based on the access policy* for the user. For the reasons stated previously with respect to Applicants' allowable independent claim 1, Applicants traverse Examiner's rejection of independent claims 8 and 13, and consider independent claims 8 and 13 to be allowable. Since claims 9-12, and 14-17, depend from allowable independent claims 8 and 13 respectively, Applicants traverse the Examiner's rejections of such dependent claims, and consider claims 9-12, and 14-17 to also be allowable as depending from allowable base claims.

CONCLUSION

Applicants consider the Response herein to be fully responsive to the referenced Office Action. Based on the above Remarks, it is respectfully submitted that this application is in condition for allowance. Accordingly, allowance is requested. If there are any remaining issues or the Examiner believes that a telephone conversation with Applicants' attorney would be helpful in expediting the prosecution of this application, the Examiner is invited to call the undersigned at (972) 718-4800.

Respectfully submitted,

Date: September 29, 2004

Joe Wall
Attorney for Applicants
Registration No. 25,648

Verizon Corporate Services Group Inc.
c/o Christian Andersen
600 Hidden Ridge, HQE03H14
Irving, TX 75038
Tel.: (972) 718-4800
CUSTOMER NO. 32127